@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Automating Incident Response

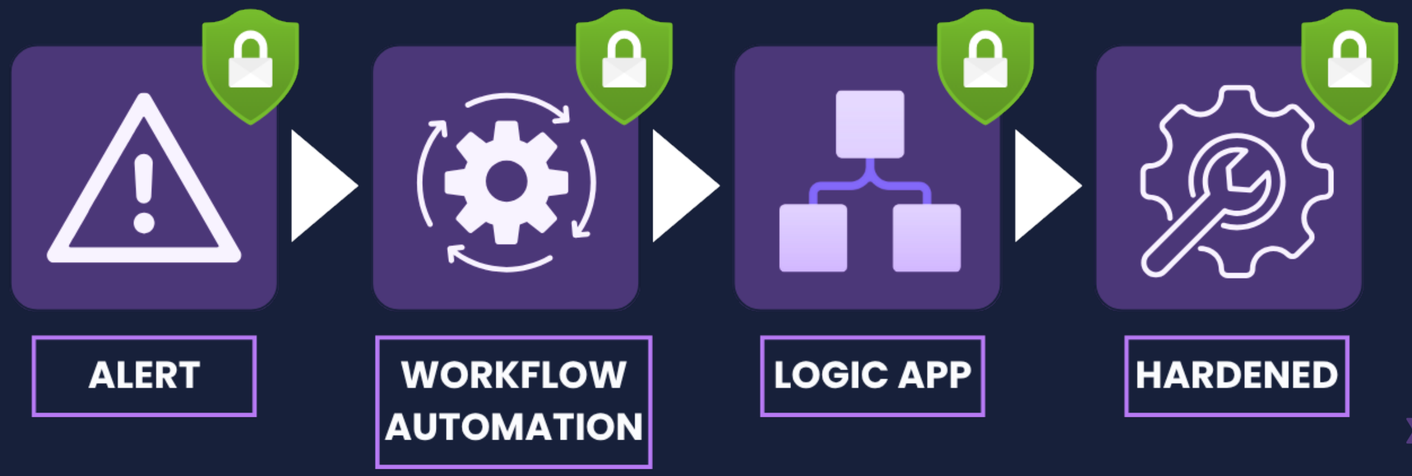
Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Automating Incident Response

- Manual remediation is slow and error-prone
- Security incidents require consistent, rapid response
- Automation ensures alerts don’t go ignored



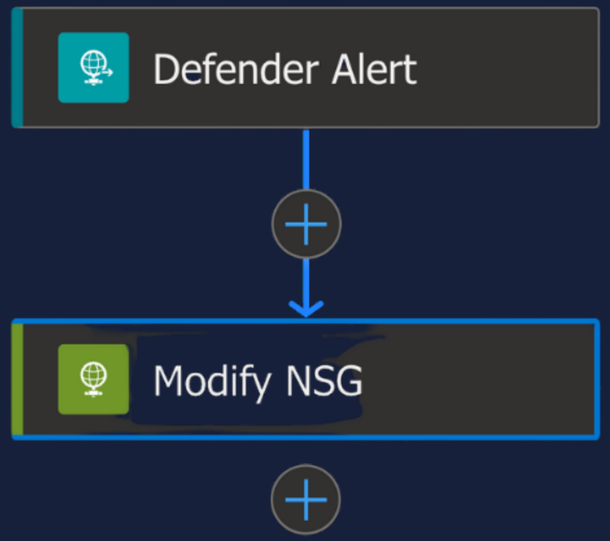
@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Microsoft Defender for Cloud

Logic App Playbook

- Logic App that executes specific remediation tasks
- Integrated with Defender for Cloud
- When defender detects a threat, connects to workflow automation rule



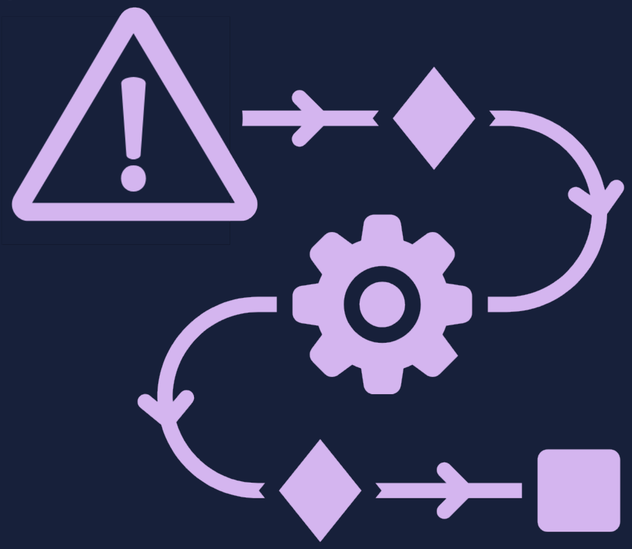
@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Microsoft Defender for Cloud

Example

- Quarantine a VM
- Email your SOC team
- Disable a compromised user
- Open a ticket in ServiceNow
- Isolate a subnet, etc.



@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

THANK YOU!